

### **REMARKS**

The Office Action dated April 9, 2008 has been received and carefully noted. Applicant appreciatively acknowledges the examination of the pending claims. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-2, 4-10, 13, 22-25, 46, and 56-71 are pending in the application. Claims 1-2, 4-10, 13, 22, 25, and 46 have been amended to more particularly point out and distinctly claim the subject matter of the invention. Claims 56-71 have been added. Support for these amendments may be found throughout the Specification, such as in paragraphs [0051]-[0054]. Claims 3, 12, 26-43, and 48-55 have been canceled without prejudice or disclaimer. No new matter is added. Applicant submits the pending claims for consideration in view of the following.

#### **§103(a) Rejections**

Claims 1-10, 22-29, 31, 33-35, 38, 39, 43, 46, and 48 were rejected under 35 U.S.C. §103(a) as being unpatentable as obvious over Jennings, *et al.* (Internet Draft, “Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks”) (hereinafter, “Jennings”) in view of Marshall, *et al.* (Internet Draft, “SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks”) (hereinafter, “Marshall”). The Office Action took the position that Jennings discloses most of the limitations of the rejections, with the exception of, for example, “modifying”

when a message has not been through a security check. In light of the deficiencies of Jennings, the Office Action relied on Marshall to support the rejection. Applicant respectfully asserts that a combination of Jennings and Marshall fails to disclose or suggest all the limitations of the rejected claims.

Claim 1, upon which claims 2, 4-10, 13, and 63-67 are dependent, is generally directed to an apparatus that includes a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer, a forwarder configured to forward the message within said first network regardless of the result of the determination, and a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check if the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer.

Claim 22, upon which claims 23-24 and 69-71 are dependent, are generally directed to a system that includes a security server and a network processing element. The security server is configured to receive a message, determine whether the message has been through a security check by determining whether or not the message has been received with security at a first layer, and, if the result of the determination is that the message has not been through a security check, modify the message so as to include a second layer indication that the message has not been through a security check. The second layer is a higher layer than said first layer. The security server may further be

configured to forward the message to the network processing element regardless of the result of the determination.

Claim 25, upon which claims 56-62 are dependent, is generally directed to a method that includes determining that a message received at a first network has not been through a security check by determining that the message has not been received with security at a first layer, modifying the message so as to include a second layer indication that the message has not been through a security check, where the second layer is a higher layer than the first layer, and forwarding the message within the first network.

Claim 46 is generally directed to an apparatus that includes determining means for determining whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer, modifying means for, if the message is determined not to have been through a security check, modifying the message to include a second layer indication that the message has not been through a security check, wherein the second layer is a higher layer than the first layer, and forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

Applicant respectfully submits that the foregoing claims recite limitations that are not disclosed by a combination of Jennings and Marshall.

Jennings discloses private extension to session initiation protocol (SIP) that enable a network of trusted SIP servers to assert the identity of end users or end systems, and the

application of existing privacy mechanisms. In Jennings, the use of the extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information.

Marshall discloses extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. Marshall discloses that the use of these extensions are only applicable inside an administrative domain, or among federations of administrative domains with previously agreed-upon policies for usage of such information.

However, a combination of Jennings and Marshall fails to disclose or suggest “a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer; a forwarder configured to forward the message within said first network regardless of the result of the determination; and a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check if the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer,” as recited in claim 1, and as analogously recited in claims 22, 25, and 46.

Instead, as mentioned above, Jennings discloses private extension to session initiation protocol (SIP) that enable a network of trusted SIP servers to assert the identity of end users or end systems, and the application of existing privacy mechanisms.

However, Jennings does not disclose that, for example, a determination is made as to whether or not a message has been received with security at a first layer, or that a message is modified to include a second layer indication depending on a determination regarding a first layer security.

Similarly, Marshall fails to disclose the foregoing limitations or otherwise remedy the deficiencies of Jennings. Instead, Marshall discloses extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems. Marshall, similar to Jennings, fails to disclose, for example, a determination is made as to whether or not a message has been received with security at a first layer, or that a message is modified to include a second layer indication depending on a determination regarding a first layer security.

Accordingly, Applicant respectfully asserts that a combination of Jennings and Marshall fails to disclose or suggest all the limitations of claims 1, 22, 25, and 46. Therefore, Applicant respectfully requests that the rejection of claims 1, 22, 25, and 46 be withdrawn. Similarly, Applicant respectfully requests that the rejection of claims requests that the rejection of claims 2, 4-9, 23-24, and 48 be withdrawn for their dependence from claims 1, 22, and 25, and for the patentable subject matter recited therein. Additionally, Applicant respectfully asserts the patentability of new claims 56-71 for similar reasons. As indicated above, claims 3, 26-29, 31, 33-35, 38-39, 42, and 48 have been canceled.

Claims 12, 30, 37, 41, and 49-55 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable as obvious over Jennings in view of Marshall as applied to claims 1, 22, 25, 26, 33, 43, 46, and 48, and further in view of Arkko, *et al.* (U.S. Patent Publication No. 2002/0052200). As indicated above, claims 12, 30, 37, 41, and 49-55 have been canceled, which renders this rejection moot. Withdrawal thereof is therefore respectfully requested.

Claims 13, 32, and 42 were rejected under 35 U.S.C. §103(a) as being unpatentable as obvious over Jennings in view of Marshall as applied to claims 1, 26, and 33, and further in view of Soininen (Internet Draft, "Transition Scenarios for 3GPP Networks") ("Soininen"). The Office Action took the position that a combination of Jennings and Marshall failed to disclose or suggest all the limitations of the rejected claims. However, the Office Action also took the position that Soininen satisfies the deficiencies of Jennings and Marshall in a manner that renders the claims 12, 30, 37, 41, and 49-55 obvious. Applicant respectfully asserts that a combination of Jennings, Marshall, and Soininen fails to disclose or suggest all the limitations of the rejected claims.

As mentioned above, Jennings discloses private extension to session initiation protocol (SIP) that enable a network of trusted SIP servers to assert the identity of end users or end systems, and the application of existing privacy mechanisms. In Jennings, the use of the extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport and usage of such information.

As also mentioned above, Marshall discloses extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. Marshall discloses that the use of these extensions are only applicable inside an administrative domain, or among federations of administrative domains with previously agreed-upon policies for usage of such information.

Soininen generally discloses different scenarios in a Third Generation Partnership Project (3GPP) defined packet network that would need IP versions 6 and IP version 4 transitions. However, Soininen, similar to Jennings and Marshall, fails to disclose or suggest “a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer; a forwarder configured to forward the message within said first network regardless of the result of the determination; and a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check if the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer,” as recited in claim 1, from which claim 13 is dependent.

Instead, Soininen discloses scenarios where the user equipment connects to nodes in other networks, e.g., the Internet. Indeed, Soininen, similar to Jennings and Marshall, does not disclose that, for example, a determination is made as to whether or not a message has been received with security at a first layer, or that a message is modified to

include a second layer indication depending on a determination regarding a first layer security. Accordingly, Applicant respectfully asserts that a combination of Jennings, Marshall, and Soininen fails to disclose or suggest all the limitations of claim 1.

Therefore, Applicant respectfully requests that the rejection of claim 13 be withdrawn for the dependency of claim 13 from claim 1, and for the patentable subject matter recited therein. Additionally, Applicant respectfully asserts the patentability of new claims 56-71 for similar reasons. As indicated above, claims 32 and 42 have been canceled.


Claims 36 and 40 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable as obvious over Jennings in view of Marshall as applied to claim 35, and further in view of Haukka (U.S. Patent Publication No. 2003/0210678). Similar to the rejection of claims 12, 30, 37, 41, and 49-55 above, claims 36 and 40 have been canceled, which renders this rejection moot. Withdrawal thereof is therefore respectfully requested.

### **Conclusion**

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

  
\_\_\_\_\_  
Jared T. Olson  
Attorney for Applicant  
Registration No. 61,058

**Customer No. 32294**  
SQUIRE, SANDERS & DEMPSEY LLP  
14<sup>TH</sup> Floor  
8000 Towers Crescent Drive  
Vienna, Virginia 22182-6212  
Telephone: 703-720-7800  
Fax: 703-720-7802

JTO:dlh/skl

Enclosures: Petition for Extension of Time  
Check No. 019395